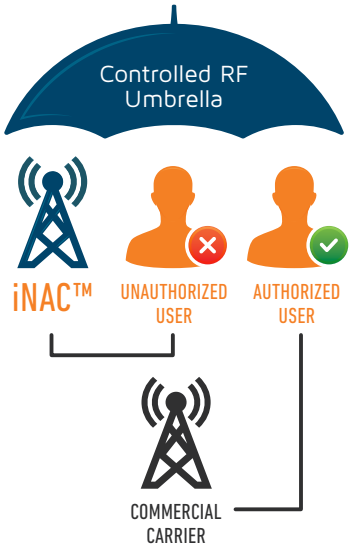
Intelligent Network Access Controller (iNAC)™

Managed Access

As the popularity and benefits of wireless communications grow, so do unwanted side effects – such as use of cellular devices in restricted areas. Recent national security events ranging from illegal activity coordinated from correctional institutions to information and security leaks from secured facilities have only emphasized the need to implement a measure of communications control in these targeted areas. Leveraging the patented technology of Managed Access as well as multiprotocol wireless operations, the Intelligent Network Access Controller (iNAC)™, forms a radio frequency umbrella around a precisely defined target area and manages cellular devices within range. iNAC Managed Access provides the system operator with the capability to selectively permit or deny communications for devices within the restricted area based on a rich policy engine that includes continued support for cellular network regulations such as 911. The iNAC does not require changes in law to operate.

ADVANTAGES of iNAC

1. Assurance that unwanted communications are being disrupted before they occur
2. Avoidance of resource-intensive measures to manually locate and retrieve devices
3. Addressing not only cell phones, but subscriber identity module (SIM) cards, which store contact lists and account plans, are as small as postage stamps and easily concealable, and can be transferred from one phone to another so that inmates can continue to place calls
4. Availability of device and call information for forensic analysis consistent with applicable law
5. Options for tracking device location
6. A range of funding options to accelerate deployments and prevent further threat to the community at large



FEATURES AND BENEFITS

- Based on the patented iCore platform, supporting multiple network technologies and commercial carriers from a single system
- Designed for fixed and mobile deployments
- Supports centralized and distributed modes of operations
- Provides local and remote management capabilities
- Purposely built for state and federal DOC facilities
- Supports 2G/3G/4G commercially deployed radio access network technologies
- Provides management of authorized and non-authorized subscribers
- Software remotely upgradeable for new feature enhancements and maintenance releases

Tecore Networks is the inventor of the patented Managed Access Technology (Patent No.: 8,254,886, 8,509,740 & 8,437,741, 6,912,230, 7,733,901 & EPA 39080, 42709)

7030 Hi Tech Drive Hanover, MD 21076, U.S.A. + 1.410.872.6500 government@Tecore.com www.Tecore.com

VALUE ADDED FEATURES

While targeted focus of the iNAC Managed Access solution is to provide the control of the cellular communications within the targeted footprint of the system, there are additional features and capabilities that can be added to the platform to expand the scope and capability of the service:

Secured Local WiFi Service

In addition to including WiFi as part of the Managed Access RF umbrella, the iNAC can be equipped to include a local facility run secured WiFi service. This capability can be used for revenue generating services as well as local inmate education, scheduling appointments, and content distribution.

Interoperability for Emergency Communications

To further assist the critical communications within the facility, the iNAC Managed Access system supports the addition of P25 radio capability. By enabling the use of the P25 capability throughout the iNAC footprint, authorized personnel can leverage the capabilities of their standard radio without installing separate infrastructure.

WiFi and Bluetooth Control

The iNAC Managed Access capability can be expanded to include the control of unlicensed wireless services. Operating in similar fashion to other technologies, the iNAC provides the ability to control/monitor use.

Enhanced Location Tracking

As an evolution to the patented managed access control the iNAC provides, the system can be equipped to support the additional capability of detection. When enabled, the service can obtain the location of any GPS enabled device whether the device has GPS enabled or not.

Technology Resilience

As the large operators move away from the second generation of wireless, Tecore's iNAC Managed Access solution is the only solution prepared for this transition.

iNAC for Corrections Facilities

Corrections institutions worldwide have been grappling with the pervasive and increasing threat to public security from prison inmates using contraband cell phones behind bars. Tens of thousands of cell phones have been confiscated across the U.S. in each of the past several years. Despite the efforts to search and seize these illegal devices the number found continues to grow by as much as 70 percent annually. Despite the increased search and seizure efforts the problem of contraband cell phones has continued to grow leaving the ever present threat to national security and public safety at the forefront of the security concerns for nearly every correctional institution from coast to coast.

Tecore's iNAC Managed Access is the industry's leading solution to combat the issue of contraband cell phones. Leveraging the patented operation of device by device control within the targeted area, the iNAC delivers comprehensive capabilities for state and federal Department of Corrections (DOC) and other government agencies to selectively control the access to the commercial wireless networks from within the facility. In deployments and demonstrations in separate regions of the U.S., iNAC systems have registered hundreds of call and message attempts per hour on average, with contraband devices being denied while authorized devices are simultaneously permitted to complete calls.

The iNAC Managed Access system has received industry support including from the FCC, CTIA, the top four U.S. commercial mobile operators, and other carriers whose networks cover corrections facilities. With this important backing, Tecore has been actively working with correctional institutions to plan and deploy systems.

As the communications environments have evolved and expanded, the need to selectively prohibit and allow users in a given area is a critical application. Whether for public safety, communications control, or other restrictive environment, a solution must be provided as an alternative to the full blocking.

Tecore networks